User's Manual

Version: 1.1

Model: NS-WIR150NE

IEEE802.11n Wireless LAN Broadband Router

Trademarks

Copyright @2010
Contents are subject to change without notice.
All trademarks belong to their respective proprietors.

Copyright Statement

THIS DOCUMENT CONTAINS OF PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THIS COMPANY. AND NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRICAL OR MECHANICAL, BY PHOTOCOPYING, RECORDING, OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF THIS COMPANY.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Table of Contents

REVISION HISTORY 1

CHAPTER 1 INTRODUCTION 2
1.1 Product Features 3
1.2 Package Contents 5
1.3 LED Indicator and Port Description 5
CHAPTER 2 PRODUCT INSTALLATION 8
2.1 Hardware Installation 8
2.2 Network Application Plan 10
CHAPTER 3 HOW TO LOGIN TO THE ROUTER 11
3.1 How to Set the Network Configurations 11
3.2 Login to the Router 14
CHAPTER 4 QUICK SETUP GUIDE 16
4.1 Setup Wizard 16
CHAPTER 5 ADVANCED SETTINGS 20
5.1 LAN Settings 20
5.2 WAN Settings 21
5.3 MAC Address Clone 24
5.4 DNS Settings 25
CHAPTER 6 WIRELESS SETTINGS 26
6.1 Basic Settings 26
6.2 Wireless Security Settings 28
6.3 Advanced Settings 32
6.4 WPS Settings 34
6.5 WDS Settings 36
6.6 Wireless Access Control 38
6.7 Connection Status 39
CHAPTER 7 DHCP SERVER 40
7.1 DHCP Settings 40
7.2 DHCP List and Binding 41
CHAPTER 8 VIRTUAL SERVER 43
8.1 Port Range Forwarding 43
8.2 DMZ Settings 45

CHAPTER 9 TRAFFIC CONTROL 47
9.1 Traffic Control 47
CHAPTER 10 SECURITY SETTINGS 49
10.1 Client Filter Settings 49
10.2 URL Filter Settings 51
10.3 MAC Address Filter 53
10.4 Prevent Network Attack 54
10.5 Remote Web Management 55
CHAPTER 11 ROUTING SETTINGS 57
11.1 Routing Table 57
CHAPTER 12 SYSTEM TOOLS 58
12.1 Time Settings 58
12.2 DDNS 59
12.3 Backup/Restore Settings 61
12.4 Restore to Factory Default Setting 63
12.5 Upgrade Firmware 64
12.6 Reboot the Router 64
12.7 Password Change 65
12.8 Syslog 66
12.9 Logout 67

APPENDIX 1 GLOSSARY 68

APPENDIX 2 QUESTIONS AND ANSWERS 70

Revision History

DATE	REVISION OF USER'S MANUAL	FIRMWARE
2006/4/7	First release (Version 1.1)	V

Chapter 1 Introduction

Thank you for purchasing NS-WIR150NE 11N Wireless Broadband Router!

NS-WIR150NE utilizes the latest IEEE802.11n standard with its wireless transmitting distance up to 6 times and transmitting rate 3 times than wireless G-products. It complies perfectly backwards with 802.11b/g standards and includes Router, Wireless AP, 4-port switch, and firewall in one. WMM enables you a comfortable journey in audio and video streaming and on-line games. It supports WDS (Wireless Distribution System) function for repeating and amplifying the signals to extend the wireless network coverage. Besides, you can shut broadcast SSID manually. It supports PBC and PIN encryption methods, IP address/Port/MAC address/Website filtering to protect your network against malicious attack.

It supports broadband control function to distribute downloading rates for each member. “Setup Wizard” was designed for less IT-savvy people to install the device easily and share the Internet quickly.

1.1 Product Features

- Includes router, wireless access point, four-port switch and firewall in one
- “Setup Wizard” enables you to connect Internet without entering administration interface
- Complies with the latest IEEE802.11n standard and IEEE802.11 b/g standards
- Increases 6 times coverage distance than 802.11g standard and reduces the dead spots in the coverage area
- Supports transmitting rate 3 times than wireless G-products
- Supports 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- Supports RTS/CTS protocol and data partitioning function
- Provides one 10/100Mbps Auto-Negotiation Ethernet WAN port
- Provides four 10/100Mbps Auto-Negotiation Ethernet LAN ports
- Supports xDSL/Cable MODEM, static and dynamic IP in community networking

- Supports MAC address/ IP address/ URL filtering
- Supports remote Web management and simple Web upgrading method
- Supports wireless Roaming technology for high-efficient wireless connections
- Supports SSID stealth mode and access control based over MAC address (up to 30 entries)
- Supports Auto MDI/MDIX
- Provides syslog to record the status of the router
- Supports auto negotiation/manual mode for 802.11b/802.11g
- Supports UPnP and DDNS
- Supports Firefox1.0, IE5.5 or above
- Supports LAN access control to the Internet
- Supports SNTP
- Supports virtual server, DMZ host
- Supports WDS wireless network extension
- Supports broadband control function
- Detachable antenna(only for NS-WIR150NE)

1.2 Package Contents

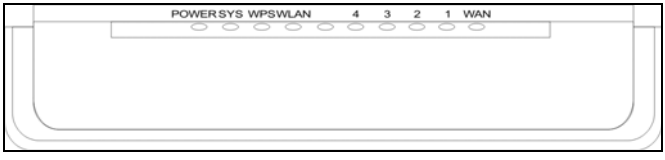
Please unpack the box and check the following items:

- One NS-WIR150NE Wireless Broadband Router
- One Quick Installation Guide
- One Power Adapter
- One CD-ROM
- One External Antenna

If any of listed items are missing or damaged, please contact the reseller from whom you purchased for replacement immediately.

1.3 LED Indicator and Port Description

Front Panel and LED Indicator Show



LED indicator description on front panel :(from L to R)

- **POWER**

  When turns green, Always ON indicates the power

connects well.

- **SYS**

  When turns green, blinking indicates the system runs well.

- **WPS**

  When blinking, it indicates the device is negotiating with client in WPS mode.

- **WLAN**

  Wireless signal LED indicator.

  When turns green, blinking indicates the wireless function is enabled.

- **LAN (4,3,2,1)**

  Wired local network LED indicator.

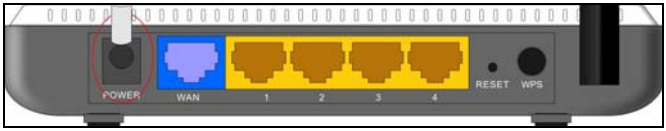
  Always ON indicates it is connected with Ethernet device; blinking indicates the device is transmitting and/or receiving data.

- **WAN**

  Wide Area Network LED Indicator.

  Always ON indicates it is connected with Ethernet device; blinking indicates the device is transmitting and/or receiving data.

Back Panel Show:



Rear Panel :(From L to R)

- **POWER**

  The jack is for power adapter connection. Please use the included 9V DC power adapter.

- **WAN**

  A 100Mbps Ethernet port can be connected with MODEM, Switch, Router and other Ethernet device for Internet connecting to DSL MODEM, Cable MODEM and ISP.

- **LAN (1, 2, 3, 4)**

  4 10/100Mbps Ethernet ports can be connected with Ethernet switch, Ethernet router and NIC card.

- **RESET**

  The system reset button. Press this button for 7 seconds, the settings configured in this device will be deleted and it will restore the settings to the default one.

- **WPS**

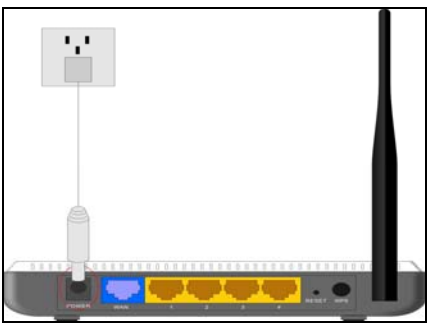
  Press it for 1 second, the WPS feature will be enabled and WPS indicator will be shown blinking.

Chapter 2 Product Installation

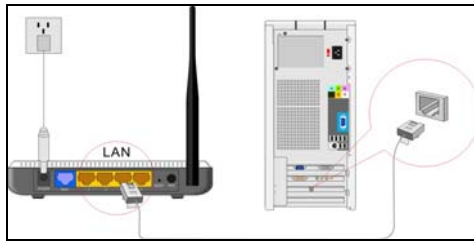
2.1 Hardware Installation

After you unpack the box, please follow the steps below to connect. For better wireless performance, please put the device in the middle of wireless coverage area.

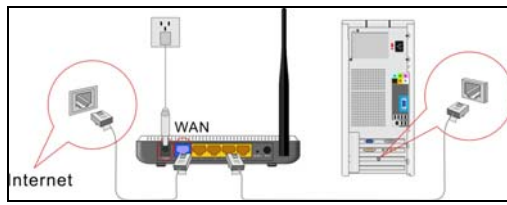
1. Please use the included power adapter to power on the Router. IMPORTANT: Use of a different power adapter could cause damage and void the warranty for this product.



2. Please connect the LAN port of the Router to the network adapter of your computer with a cable.



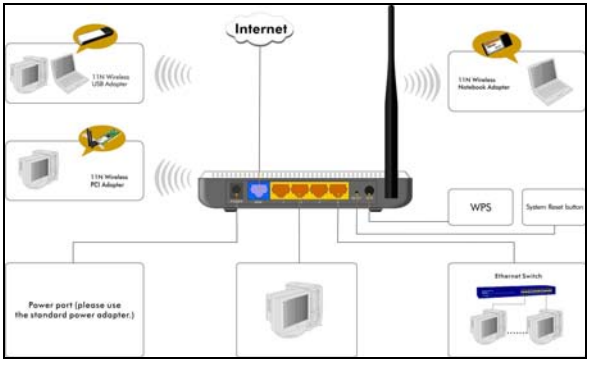
3. Please connect your broadband line provided by your ISP to the WAN port.



4. Insert the included CD-ROM into the CD-ROM drive, double click the “Setup” icon and follow the instructions to complete the installation. Or you can enter the Router’s Web page to configure it. (More details please refer to Chapter 3.)

2.2 Network Application Plan

Usually wireless LAN Network is deployed in a planned environment where each access point is located in a steady place with certain wireless coverage area for communication service. Generally speaking, it is in the center of the area to reduce “dead spot”.

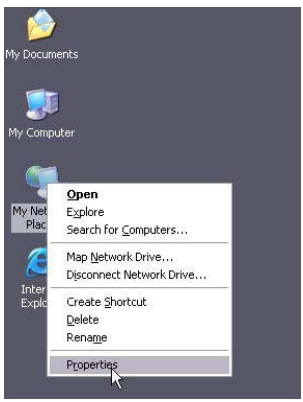


Chapter 3 How to Login to the Router

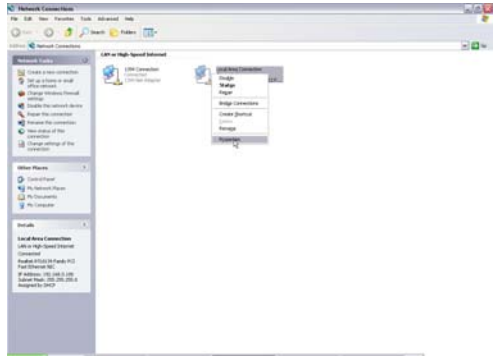
The chapter mainly presents how to enter the Router's Web page. After you have finished the hardware installation, the following steps will assist you to set the network configurations for your computer.

3.1 How to Set the Network Configurations

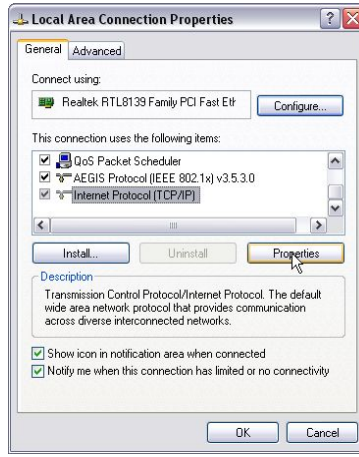
1. On your computer desktop right click "My Network Places" and select "Properties".



2. Right click “Local Area Network Connection” and select “Properties”.



3. Select “Internet Protocol (TCP/IP)” and click “Properties”.



4. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Click “OK” to save the configurations.

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

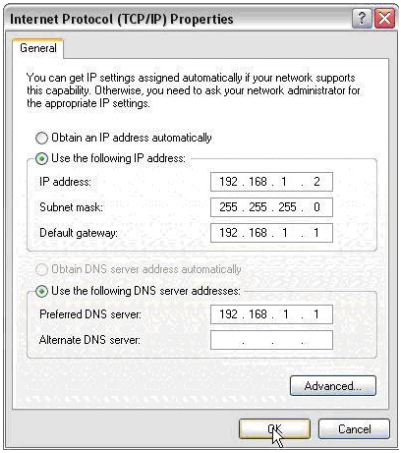
Or select “Use the following IP address” and enter the IP address, Subnet mask, Default gateway as follows:

IP Address: 192.168.1.XXX: (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

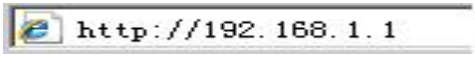
Gateway: 192.168.1.1

Certainly you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click “OK” to save the configurations.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

3.2 Login to the Router

1. To access the Router's Web-based interface, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, http://192.168.1.1. Press "Enter".



2. Input the “admin” in both User Name and Password. Click “OK”.

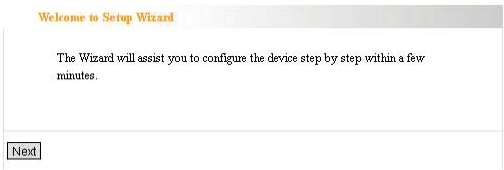
3. If you enter the correct user name and password, the screen will be the next one.

Chapter 4 Quick Setup Guide

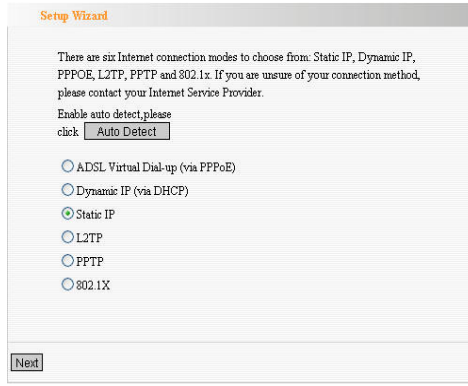
This chapter deals with how to access the Internet quickly. Please follow this guide to connect your Router to the Internet.

4.1 Setup Wizard

Here is the “Welcome to Setup Wizard” for configuring your Router quickly. Click “Next”.



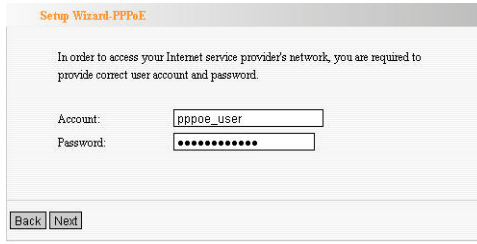
In this screen, select one mode of your Internet connection you use. If you are not clear, press the “Detect” button or contact your Internet Service Provider, and click “Next”.


Setup Wizard
There are six Internet connection modes to choose from: Static IP, Dynamic IP, PPPOE, L2TP, PPTP and 802.1x. If you are unsure of your connection method, please contact your Internet Service Provider.
Enable auto detect,please click
Auto Detect
ADSL Virtual Dial-up (via PPPoE)
Dynamic IP (via DHCP)
Static IP
L2TP
PPTP
802.1X
Next

ADSL Virtual Dial-up (Via PPPoE)

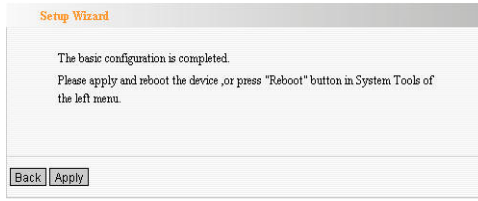
Enter the Account and Password provided by your ISP, and click “Next”.

For example:



Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like other modes. Click “Next” and “Save” to finish the settings.


Setup Wizard
The basic configuration is completed.
Please apply and reboot the device ,or press "Reboot" button in System Tools of the left menu.
Back
Apply

Static IP

In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click “Next”.

For example:

ISP provides the following TCP/IP parameters as follows:

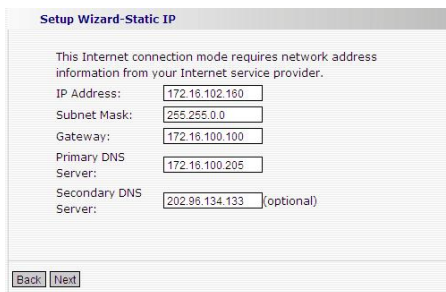
IP Address: 172.16.102.160

Subnet Mask: 255.255.0.0

Gateway: 172.16.100.100

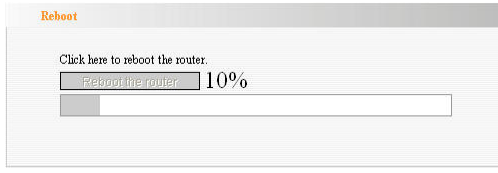
Primary DNS Server: 172.16.100.205

Alternate DNS Server: 202.96.134.133

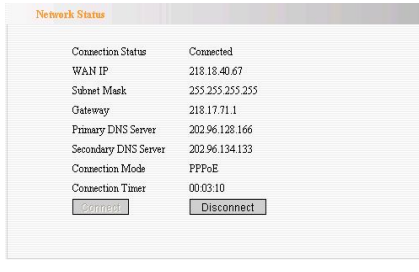


Click “Save” to complete the setup wizard. The Router

will record the settings you made. To activate the settings, it is recommended to select “Reboot the Router” from “System Tool” of the left menu. It is rebooting now, please wait for a few minutes and DO NOT power off it.



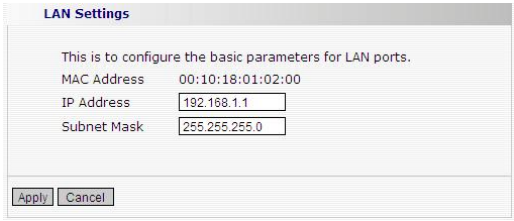
Click the “System Status” in the left menu of the Web-based Utility to find out the current network and system information. If the “Connection Status” is “Connected”, Congratulations you on completing the Router’s basic settings. You are on the Internet now. If you want to configure more, please proceed to the following explanations for Advanced Settings.



Chapter 5 Advanced Settings

5.1 LAN Settings

LAN Settings are for the basic TCP/IP parameters of LAN ports.



- **MAC Address:** The Router's physical MAC address as seen on your local network, which is unchangeable.
- **IP Address:** The Router's LAN IP addresses (not your PC's IP address). 192.168.1.1 is the default value.
- **Subnet Mask:** It's shown the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value.

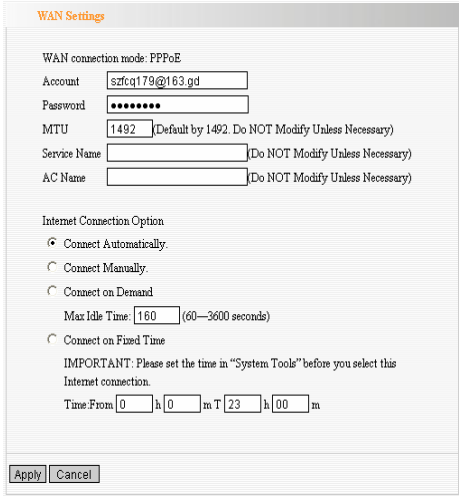
IMPORTANT:

Once you modify the IP address, you need to remember it for the Web-based Utility login next time.

5.2 WAN Settings

After you have selected the ISP connection type in "Setup Wizard" and you want to modify the related settings, here you can modify and configure the settings in details.

Virtual Dial-up (PPPoE)



- **Connection Mode:** Show your current connection mode.
- **Account:** Enter them provided by your ISP.
- **Password:** Enter them provided by your ISP.
- **MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network.

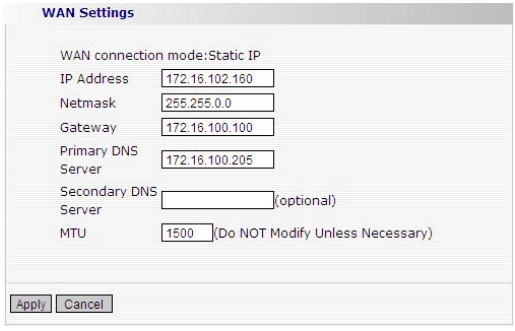
The default value is 1492. Do NOT modify it unless necessary. But if when some specific website or web application software can not be open or enabled, have a try to change the MTU value as 1450, 1400, etc.

- **Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- **AC Name:** Enter it if provided. Do NOT modify it unless necessary.
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect Manually:** Connect to the Internet by users manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix.

Notice:

The “Connect on Fixed Time” can be deployed only when you have set the current time in “Time Settings” from “System Tools”.

Static IP

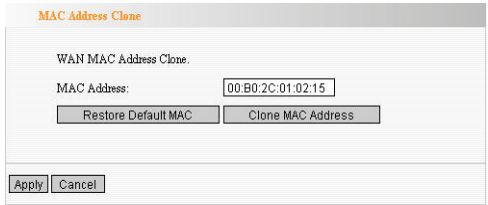


If your connection mode, static IP is chosen, you can modify the following addressing information.

- **IP Address:** Here enter the WAN IP address provided by your ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask here.
- **Gateway:** Enter the WAN Gateway here.
- **Primary DNS Server:** Enter the Primary DNS server provided by your ISP.
- **Secondary DNS Server:** Enter the secondary DNS.

5.3 MAC Address Clone

This page is for the Router's MAC address to WAN.

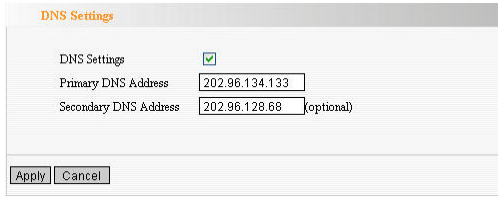


Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

- **MAC Address:** The MAC address to be registered with your Internet service provider.
- **Clone MAC Address:** Register your PC's MAC address.
- **Restore Default MAC Address:** Restore to the default hardware MAC address.

5.4 DNS Settings

DNS is short for Domain Name System (or Service), an Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.



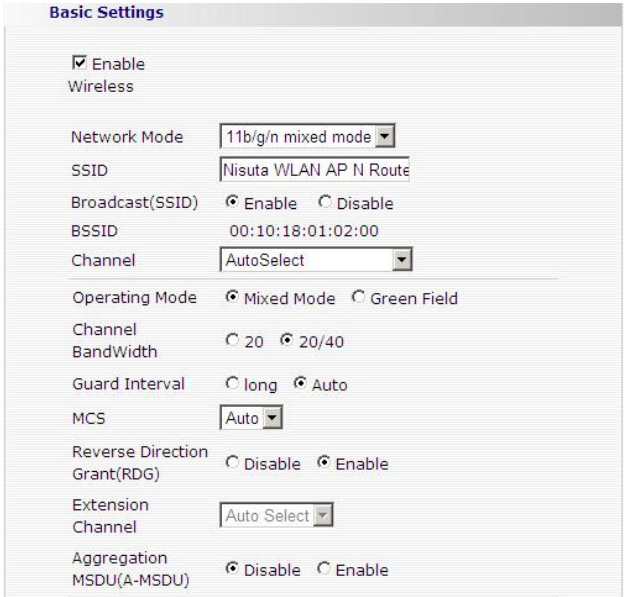
- **DNS:** Click the checkbox to enable the DNS server. The Router's DHCP sever will answer the client's requests and distribute DNS address.
- **Primary DNS Address:** Enter the necessary address provided by your ISP.
- **Secondary DNS Address:** Enter the second address if your ISP provides, which is optional.

Notice:

After the settings are completed, reboot the device to activate the modified settings.

Chapter 6 Wireless Settings

6.1 Basic Settings



- **Enable Wireless:** Check to enable the Router's wireless features; uncheck to disable it. You can also press the WLAN/WPS button to turn on/off the wireless function.
- **Network Mode**: Select one mode from the following. The default is 11b/g/n mode.

  11b mode: Allow the wireless client to connect

with the device in 11b mode at the maximum speed of 11Mbps.

11g mode: Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

11b/g mode: Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.

11b/g/n mode: Allow 11b/g/n-compliant client device to connect with the AP with auto-negotiation speed.

- **Main SSID:** SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- **Broadcast (SSID):** Select “Enable” to enable the device's SSID to be visible by wireless clients. The default is enabled.
- **BSSID**: Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- **Channel:** Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- **Extension Channel:** To increase data throughput of wireless network, the extension channel range is used in 11n mode.

- **Channel Bandwidth:**Select the channel bandwidth to improve the wireless performance. When the network has 11b/g and 11n clients, you can select the 40M; when it is an 11n network, select 20/40M to improve its throughput.

6.2 Wireless Security Settings

It is used to configure the AP network's security setting. Here presents the common six (ten in all) encryption methods, including Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window:

- **Select SSID:**Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **Security Mode:**From the drop-down menu select the corresponding security encryption modes.
- **WEP Key1~4:**Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.
- **Default Key:**Select one key from the four configured keys as the current available one.

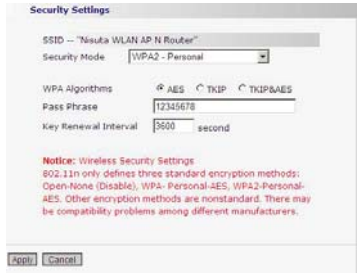
6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.

- **WPA Algorithms:**Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Pass Phrase:**Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval:**Set the key's renewal period.

6.2.3 WPA2- Personal

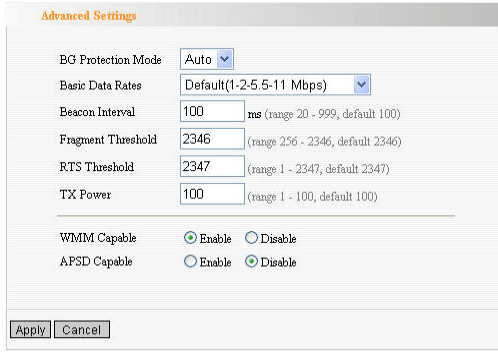
WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access).



- **WPA Algorithms:**Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Pass Phrase:**Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval:**Set the key's renewal period.

6.3 Advanced Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, etc.



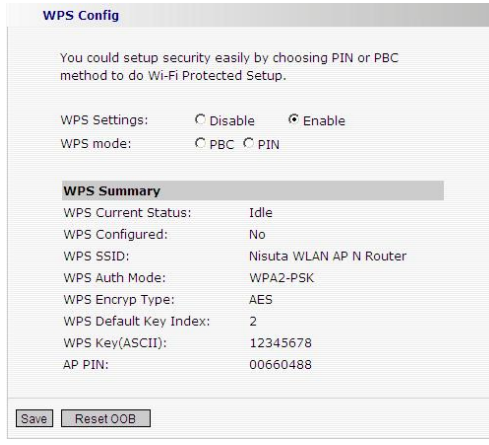
- **BG protection Mode:** Auto by default. It is for 11b/g wireless client to connect 11n wireless network smoothly in a complicated wireless area.
- **Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Here, default value is (1-2-5.5.-11Mbps…). It is recommended not to modify this value.
- **Beacon Interval:** Set the beacon interval of wireless radio. Default value is 100. It is recommended not to modify this value.
- **Fragment Threshold:** The fragmentation

threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes. It is recommended not to modify this value.

- **RTS Threshold:** RTS stands for “Request to Send”. This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2346. It is recommended not to modify this value in SOHO environment.
- **TX Power:** Set the output power of wireless radio. The default value is 100.
- **WMM Capable:** It will enhance the data transfer performance of multimedia data when they’re being transferred over wireless network. It is recommended to enable this option.
- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

6.4 WPS Settings

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the device through encrypted contents. The users only enter PIN code or press WLAN/WPA button on the panel to configure it without selecting encryption method and secret keys by manual. In the “Wireless settings” menu, click “WPS settings” to enter the next screen.


WPS Config
You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.
WPS Settings: Disable Enable
WPS mode: PBC PIN
WPS Summary
WPS Current Status: Idle
WPS Configured: No
WPS SSID: Nisuta WLAN AP N Router
WPS Auth Mode: WPA2-PSK
WPS Encryp Type: AES
WPS Default Key Index: 2
WPS Key(ASCII): 12345678
AP PIN: 00660488
Save
Reset OOB

- **WPS settings**: To enable or disable WPS function. The default is “disable”.
- **WPS mode:** Provide two ways: PBC (Push-Button Configuration) and PIN code.
- **PBC:** Select the PBC or press the WLAN/WPS button on the front panel of the device for about

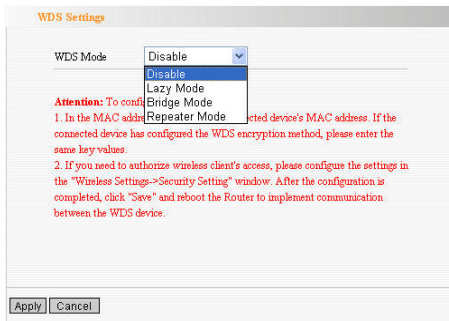
one second (Press the button for about one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports up to 32 clients access.)

- **PIN:** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client.
- **WPS Summary:** Show the current state of Wi-Fi protected setting, including authorized mode, encryption type, default key and other information.
- **WPS Current Status:** Idle means WPS in idle state. Start MSC process means the process has been started and waits for being connected. Configured means the negotiation is successful between server and clients.
- **WPS Configured:** "yes" means WPS feature is enabled and goes into effect. "not used" means it is not used. Usually the AP-security has been enabled, here will displayed "not used".
- **WPS SSID:** Show the main SSID set by WPS.
- **WPS Auth. Mode:** The authorization mode deployed by WPS, generally WPA/WPA2-personal mode.

- **WPS Encrypt Type:** The encryption type used by WPS, generally AES/TKIP.
- **WPS key:** The effective key generated by AP automatically.
- **AP PIN(KEY):** The PIN code used by default.
- **Reset OOB:** When this button is pressed, the WPS client will be idle state, and WPS indicator will be turned off. AP will not respond the WPS client's requests and the set the security mode as WPA mode.

6.5 WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.


WDS Settings
WDS Mode
Disable
Disable
Lazy Mode
Bridge Mode
Repeater Mode
Attention: To confi
cted device's MAC address. If the
connected device has configured the WDS encryption method, please enter the
same key values.
2. If you need to authorize wireless client's access, please configure the settings in
the "Wireless Settings->Security Setting" window. After the configuration is
completed, click "Save" and reboot the Router to implement communication
between the WDS device.
Apply
Cancel

Lazy: In this mode, the connected device can be Bridge mode or Repeater mode and enter the Router's BSSID

to establish the connection.

Bridge: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table.

Repeater Mode: In this mode, add the opposing MAC address into each own AP MAC address table by manual or scanner to enlarge and extend the wireless radio.

Encrypt Type: Select one from WEP, TKIP, AES for security here.

Pass phrase: Enter the encrypted key for wireless devices.

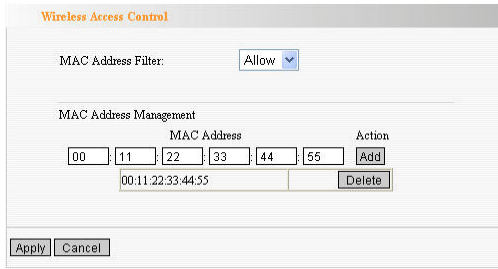
AP MAC: Input the MAC address of another (opposing) wireless router you want to connect.

⚠**NOTE:**

It is recommended that two wireless routers keep the same bandwidth, channel number, and security settings. Apply the settings and reboot the Router to activate it.

6.6 Wireless Access Control

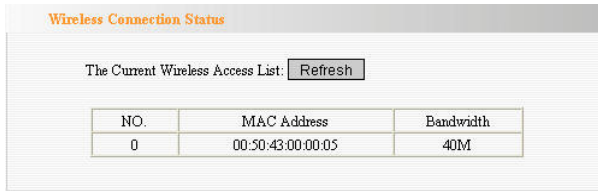
To secure your wireless LAN, the wireless access control is actually based on the MAC address management to allow or block the specific clients to access the wireless network. Select “Wireless Setting->Access Control” to display the following screen:



- **MAC Address Filter:** Enable/disable MAC address filter. Select “Close” to malfunction MAC address; “disable” to prevent the MAC addresses in the list from accessing the wireless network; “Allow” to allow the MAC address in the list to access the wireless network.
- **MAC Address Management:** Input the MAC address to implement the filter policy. Click “Add” to finish the MAC add operation.
- **MAC list:** Show the added MAC addresses. You can add or delete them.

6.7 Connection Status

This page shows wireless client's connection status, including MAC address, Channel bandwidth, etc. Select "Wireless Setting->connection status" to enter the following screen:

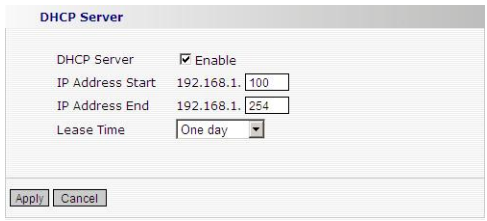


- **MAC Address:** Shows current MAC addresses of the hosts connecting to the Router.
- **Bandwidth:** Shows current bandwidth of the hosts (wireless client).

Chapter 7 DHCP Server

7.1 DHCP Settings

DHCP (Dynamic Host Control Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating “Obtain an IP Address Automatically”. So specifying the starting and ending address of the IP Address pool is needed.



- **DHCP Server:** Activate the checkbox to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP address for DHCP server distribution.
- **Lease Time:** The length of the IP address lease.

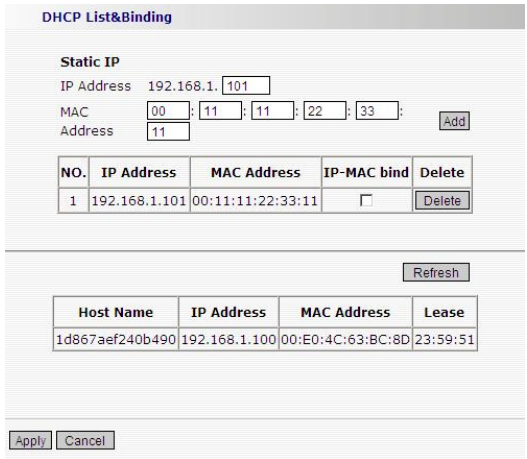
For example:

If the lease time is an hour, then DHCP server will

reclaim the IP address each hour.

7.2 DHCP List and Binding

The Static IP assignment is to add a specifically static IP address to the assigned MAC address. You can view the related information in the DHCP server list.


DHCP List&Binding
Static IP
IP Address 192.168.1. 101
MAC Address 00 : 11 : 11 : 22 : 33 : 11
Add
NO. IP Address MAC Address IP-MAC bind Delete
1 192.168.1.101 00:11:11:22:33:11 Delete
Refresh
Host Name IP Address MAC Address Lease
1d867aef240b490 192.168.1.100 00:E0:4C:63:BC:8D 23:59:51
Apply Cancel

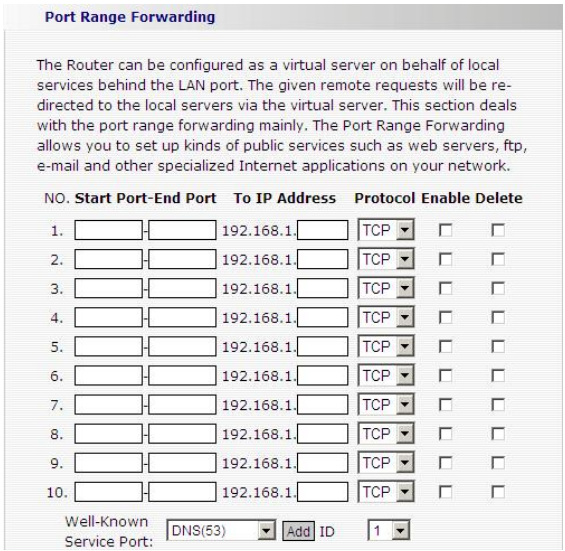
- **IP Address:** Enter the IP address which needs to be bound.
- **MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click “Add” to add the entry in the list.
- **Hostname:** The name of the computer which is added a new IP address.
- **Lease Time:** The left time length of the

corresponding IP address lease.

Chapter 8 Virtual Server

8.1 Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.


Port Range Forwarding
The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.
NO. Start Port-End Port To IP Address Protocol Enable Delete
1. 192.168.1. TCP
2. 192.168.1. TCP
3. 192.168.1. TCP
4. 192.168.1. TCP
5. 192.168.1. TCP
6. 192.168.1. TCP
7. 192.168.1. TCP
8. 192.168.1. TCP
9. 192.168.1. TCP
10. 192.168.1. TCP
Well-Known Service Port: DNS(53) Add ID 1

- **Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.

- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Add:** Add the selected well-known port to the policy ID.

For example:

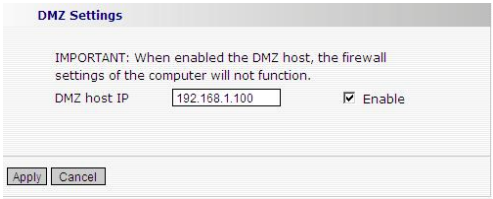
The server at IP address of 192.168.1.10 provides WEB service for port 80 and Telnet service for port 23. If you want clients in the Internet visit that server, you need to set it as above.

⚠**NOTE:**

If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.2 DMZ Settings

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.



- **DMZ Host IP Address:** The IP address of the computer you want to expose.
- **Enable:** Click the checkbox to enable the DMZ host.

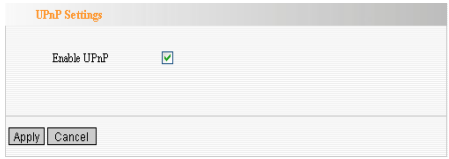
For example:
Set the computer at IP address of 192.168.1.100 as DMZ host to connect another host in the Internet for intercommunication.

IMPORTANT: When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

8.3 UPNP Settings

It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this

function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.

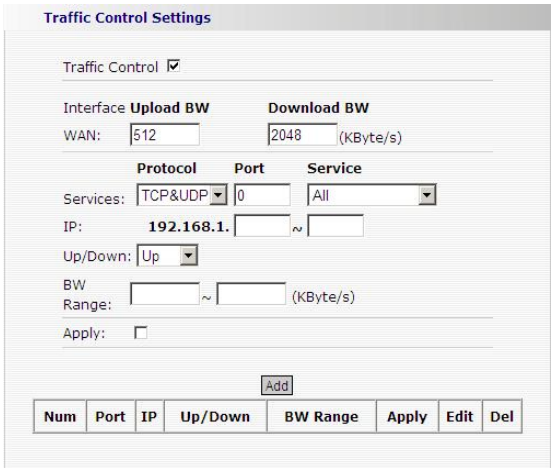


- **Enable UPnP:** Click the checkbox to enable the UPnP.

Chapter 9 Traffic Control

9.1 Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.



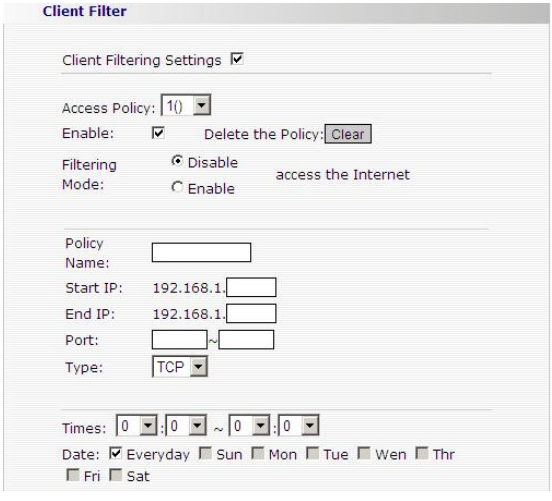
- **Enable Traffic Control:** To enable or disable the internal IP bandwidth control. The default is disabled.
- **Interface:** To limit the uploading and downloading bandwidth in WAN port.

- **Service:** To select the controlled service type, such as HTTP service.
- **IP Starting Address:** The first IP address for traffic control.
- **IP Ending Address:** The last IP address for traffic control.
- **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- **Bandwidth:** To specify the uploading/downloading Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.
- **Apply:** To enable the current editing rule. If not, the rule will be disabled.
- **Add:** After edit the rule, click the “add to list” button to add the current rule to rule list.
- **Apply:** Click “Save” to activate the current rule.
- **Cancel:** Click “Cancel” to drop all setting saved last time.

Chapter 10 Security Settings

10.1 Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.



- **Client Filter:** Check to enable client filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click “Clear” button to clear all settings for the policy.

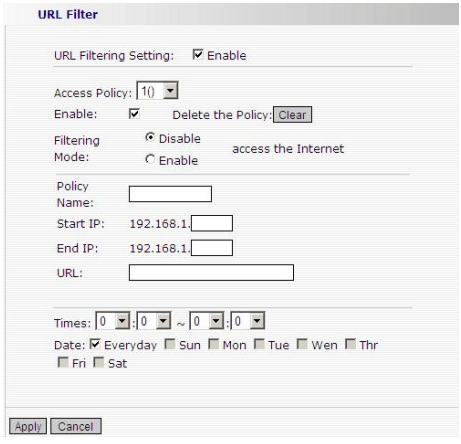
- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **IP Start/End:** Enter the starting/ending IP address.
- **Port No:** Enter the port range based over the protocol for access policy.
- **Protocol:** Select one protocol (TCP/UDP/Both) from the drop-down menu.
- **Times:** Select the time range of client filter.
- **Date:** Select the day(s) to run the access policy.

For example:

If you don't want the designated computer at IP address of 192.168.1.10 to visit website from 8:00 to18:00 everyday without restriction to other computers, you need to set it as above.

10.2 URL Filter Settings

In order to control the computer to have access to websites, you can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.



- **URL Filter:** Check to enable URL filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or

disable to access the Internet.

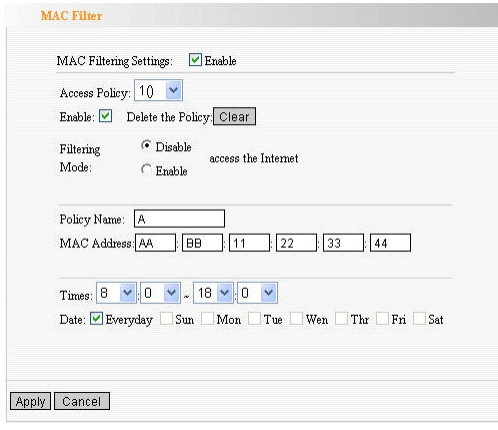
- **Policy Name:** Enter a name for the access policy selected.
- **Start/End IP:** Enter the starting/ending IP address.
- **URL Strings:** Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.
- **Times:** Select the time range of client filter.
- **Date:** Select the day(s) to run the access policy.
- **Save:** Click “Save” to activate the configuration.

For example:

If you don’t want the computer at IP address of 192.168.1.11 to visit the website contained “sex” and “game”, you need to set it as above.

10.3 MAC Address Filter

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.


MAC Filter
MAC Filtering Settings: Enable
Access Policy: 10
Enable: Delete the Policy: Clear
Filtering Mode: Disable Enable access the Internet
Policy Name: A
MAC Address: AA BB 11 22 33 44
Times: 8 : 0 ~ 18 : 0
Date: Everyday Sun Mon Tue Wen Thr Fri Sat
Apply Cancel

- **MAC Address Filter:** Check to enable MAC address filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click "Clear" button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy

selected.

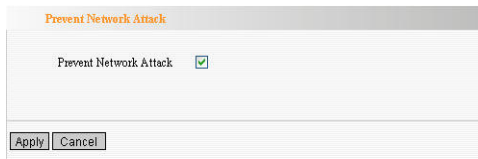
- **MAC Address:** Enter the MAC address you want to run the access policy.
- **Times:** Select the time range of client filter.
- **Date:** Select the day(s) to run the access policy.
- **Apply:** Click to make the settings go into effect.

For example:

If you want to configure the host with MAC address 00:C0:9F:AD:FF:C5 not to access the Internet at 8:00-18:00, you need to set it as above.

10.4 Prevent Network Attack

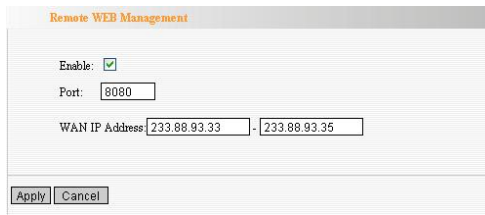
This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically.
The attacker's IP address can be found from the "System Log".



- **Prevent Network Attack:** Check to enable it for attack prevention.

10.5 Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the "Enable".



- **Enable:** Check to enable remote web management.
- **Port:** The management port open to outside access. The default value is 80.
- **WAN IP Address:** Specify the range of the WAN IP address for remote management.

Note:

1. If you want to login the device's Web-based interface via port 8080, you need use the format of WAN IP address: port (for example http://233.93.88.33: 8080) to implement remote login.

2. If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 233.88.93.33-233.88.93.35, then only the IP addresses as 233.88.93.33, 233.88.93.34 and 233.88.93.35 can access the Router.

For example:

If you want to configure the IP address 233.88.93.33 to access the device's web interface, please set it as above.

10.6 WAN Ping

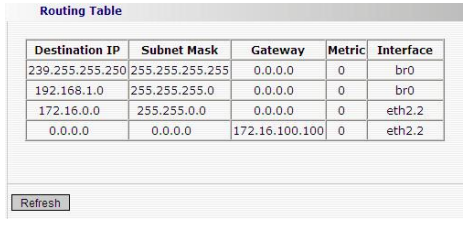
The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.

- **Ignore Ping from WAN:**
  Check to ignore the ping request and give no reply.

Chapter 11 Routing Settings

11.1 Routing Table

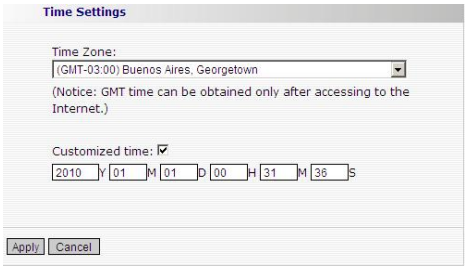
The main duty for a router is to look for a best path for every data frame, and transfer this data frame to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.



Chapter 12 System Tools

12.1 Time Settings

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.


Time Settings
Time Zone:
(GMT-03:00) Buenos Aires, Georgetown
(Notice: GMT time can be obtained only after accessing to the Internet.)
Customized time:
2010 Y 01 M 01 D 00 H 31 M 36 S
Apply
Cancel

- **Time Zone:** Select your time zone from the drop-down menu.
- **Customized time:** Enter the time you customize.

Note:

When the Router is powered off, the time setting will be lost. Before the Router will obtain GMT time automatically, you need connect with the Internet and obtain the GMT time, or set the time on this page first. Then the time in other features (e.g. firewall) can be activated.

12.2 DDNS

The DDNS (Dynamic Domain Name System) is supported in this Router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select “Enable” and a DDNS service provider to sign up.

- **Main Features:**

  Owing to ISP most times provides dynamic IP address, DDNS is used to capture the changeable IP address and match the fixed domain. Then users can have access to the Internet to communicate with others.

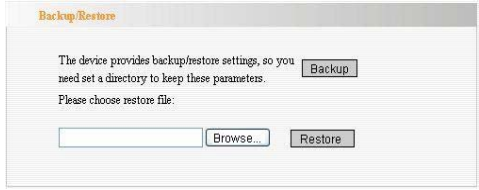
  DDNS can help you establish virtual host in your home and company.

- **DDNS:** Click the radio button to enable or disable the DDNS service.

- **Service Provider:** Select one from the drop-down menu and press “Sign up” for registration.
- **User Name:** Enter the user name the same as the registration name.
- **Password:** Enter the password you set.
- **Domain Name:** Enter the domain name which is optional.

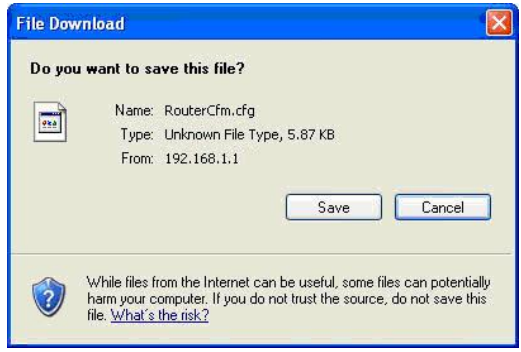
12.3 Backup/Restore Settings

The device provides backup/restore settings, so you need set a directory to keep these parameters.



- **Backup Setting:**

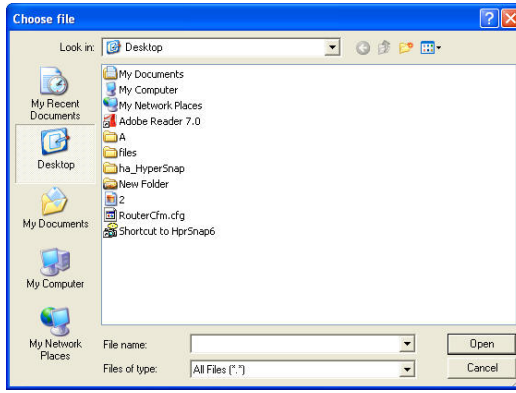
  Click “Backup” button to back up the Router’s settings and select the path for save.


File Download
Do you want to save this file?
Name: RouterCfm.cfg
Type: Unknown File Type, 5.87 KB
From: 192.168.1.1
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

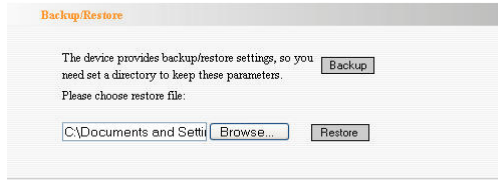
Click “Save” to save the configuration files.

➢ **Restore Setting:**

Click “Browse” button to select the backup files.

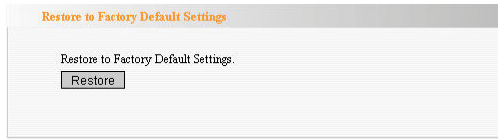


Click “Restore” button to restore previous settings.



12.4 Restore to Factory Default Setting

This button is to reset all settings to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.



- **Restore:** Click this button to restore to default settings.

- **Factory Default Settings:**
  User Name: admin
  Password: admin
  IP Address: 192.168.1.1
  Subnet Mask: 255.255.255.0

⚠ **NOTE:**

After restoring to default settings, please restart the device, then the default settings can go into effect.

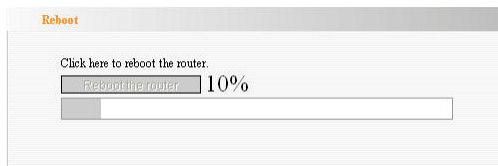
12.5 Upgrade Firmware

The Router provides the firmware upgrade by clicking the “Upgrade” after browsing the firmware upgrade packet which you can download from www.xxx.com.

- **Browse:** click this button to select the upgrade file.
- **Upgrade:** click this button to start the upgrading process. After the upgrade is completed, the Router will reboot automatically.

12.6 Reboot the Router

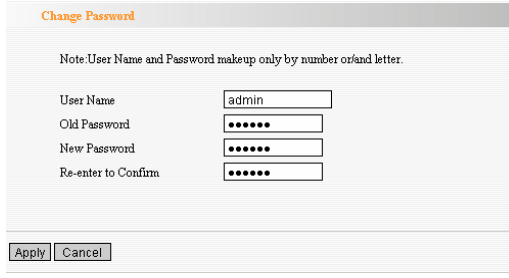
Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.



Reboot the router: Click this button to reboot the device.

12.7 Password Change

This section is to set a new user name and password to better secure your router and network.



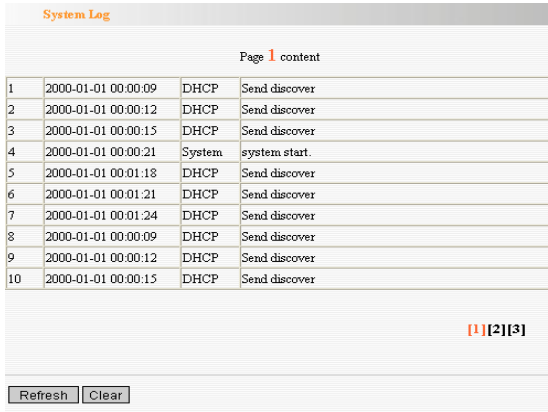
- **User Name:** Enter a new user name for the device.
- **Old Password:** Enter the old password.
- **New Password:** Enter a new password.
- **Re-enter to Confirm:** Re-enter to confirm the new password.

⚠**NOTE:**

It is highly recommended to change the password to secure your network and the Router.

12.8 Syslog

The section is to view the system log. Click the "Refresh" to update the log. Click "Clear" to clear all shown information. If the log is over 150 records, it will clear them automatically.


System Log
Page 1 content
1 2000-01-01 00:00:09 DHCP Send discover
2 2000-01-01 00:00:12 DHCP Send discover
3 2000-01-01 00:00:15 DHCP Send discover
4 2000-01-01 00:00:21 System system start.
5 2000-01-01 00:01:18 DHCP Send discover
6 2000-01-01 00:01:21 DHCP Send discover
7 2000-01-01 00:01:24 DHCP Send discover
8 2000-01-01 00:00:09 DHCP Send discover
9 2000-01-01 00:00:12 DHCP Send discover
10 2000-01-01 00:00:15 DHCP Send discover
[1][2][3]
Refresh
Clear

- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the current shown log.

12.9 Logout

After you have finished the settings completely, in logout page click “Yes” to logout the web management page.

Appendix 1 Glossary

Channel:

An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID:

SSID(Service Set Identifier) is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP:

Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are

the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommended using.

WPA / WPA2 Encryption:

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

Appendix 2 Questions and Answers

In this part some questions and problems shown during the Router's usage and installation will be given suggesting answers. If your problems are not in the list, please log into our website www.asiarf.com or send an E-mail to support@asiarf.com, and we will reply you in the first time.

1. Cannot login to the Web interface of the Router after you enter the IP address in the address field?

Step 1: check the Router if it works well. Once the device is powered on for a few seconds, the SYS indicator on the panel will be turned on. If it is not, please contact us.

Step 2: check the network cables if it is good and the corresponding indicator is "Always ON". Sometimes, the indicator is "Always ON", but it does not mean it gets through.

Run "Ping" command and check if it can ping the Router's LAN IP address 192.168.1.1. If it is OK, please make sure your browser does not access the Internet by proxy server. If the ping fails, you can press the "RESET"

button for 7 seconds to restore to default settings. And then repeat the ping operation. If it still does not work, please contact us.

2. Forget the login password and cannot enter the setting page. What can I do?

Press the “RESET” button for 7 seconds to restore the Router to default settings.

3. The computer connected with the Router shows IP address conflict. What can I do?

Check if there are other DHCP servers in the LAN. If there have, disable them. The default IP address of the Router is 192.168.1.1 and please maker sure the address is not occupied by other devices. If there are two computers with the same IP addresses, please modify one.

4. I cannot use E-mail and access the Internet. What can I do?

It happens in ADSL connection and Dynamic IP users. And you need modify the default MTU value (1492). Please in the “WAN Setting” modify the MTU value with

the recommended value as 1450 or 1400.

5. How can I configure and access the Internet via Dynamic IP?

In Setup Wizard of the Web utility interface, select “Dynamic IP” connection type and click “Save” to activate it. As some ISPs bind the user computer’s MAC address, you need to clone the Router’s WAN MAC address to the bind21ing PC’s MAC address. Select “MAC Address Clone” in “Advanced Setting” to input your computer’s MAC address and click “Apply” to activate it.

6. How to share my computer’s source with other users in Internet?

If you want Internet users to access the internal server via the Router such as e-mail server, Web, FTP, you can configure the “Virtual Server” to come true.

Step 1: create your internal server, make sure the LAN users can access these servers and know related service port. For example, Web server’s port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: in the Router’s web click “Virtual Server” and select “Single Port Forwarding”.

Step 3: input the external service port given by the Router, for example, 80.

Step 4: input the internal Web service port, for example, 80.

Step 5: Input the internal server's IP address. If your Web server's IP address is 192.168.1.10, please input it.

Step 6: select the communication protocol used by your internal host: TCP, UDP, ICMP.

Step 7: click "Apply" to activate the settings.

The following table has listed the well-known application and service port:

Server	Protocol	Service Port
WEB Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503.1720
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice:1863.6901(TCP) Voice:1863.5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110